RSAC 2025 Conference

Many Voices.
One Community.

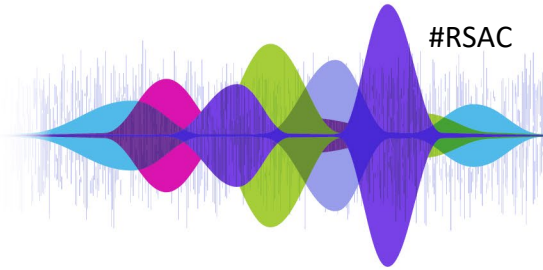
SESSION ID: GRC-M03

Imperfect Information: Embracing Uncertainty to Make Better Risk Decisions

Christopher Lau

Director, Cybersecurity and IoT Risk
Advocate Health
www.linkedin.com/in/christopher-lau-mba

Disclaimer

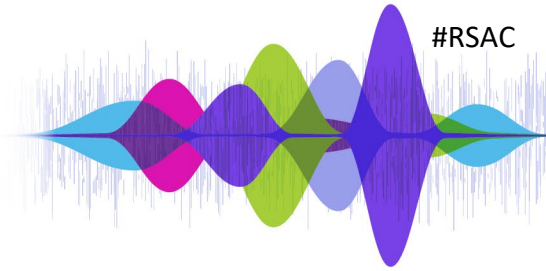


Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

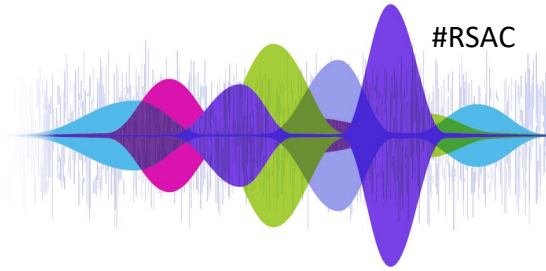
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Imperfect Information: Agenda



- Traditional Risk Mindset
- Embracing Uncertainty & Thinking Like an Attacker
- Playing Offense – Shifting to Proactive Security and Building Resiliency
- Application



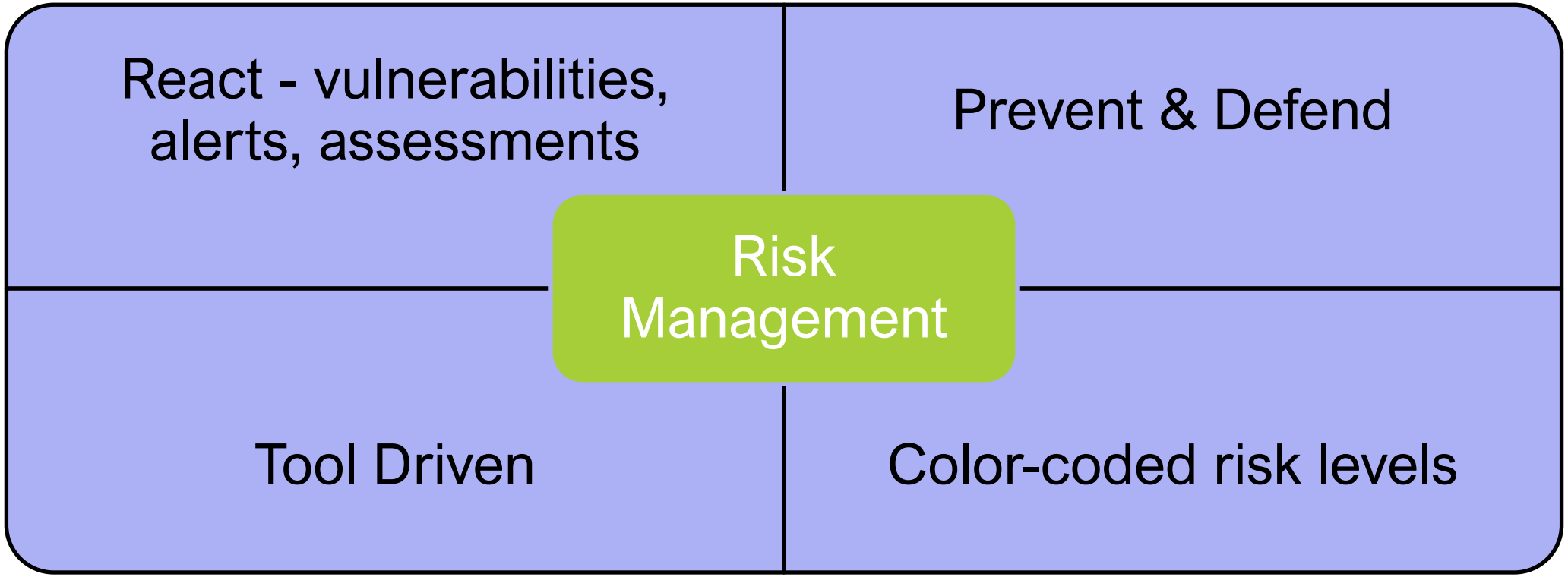
“It ain’t what you don’t know that gets you into trouble. It’s what you know for sure that just ain’t so.”

Mark Twain

RSAC™ 2025 Conference

Traditional Risk Mindset

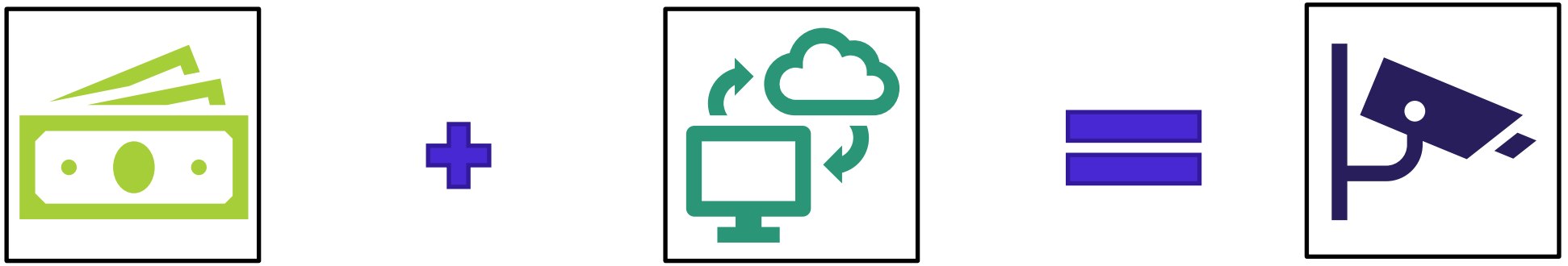
How we think about risk



Continuing the status quo combined with an ever-evolving threat landscape, risk and security teams will quickly find themselves understaffed, under-skilled, and overwhelmed.

More Money = Better Protection?

Companies increased cybersecurity spending to **$184B** in 2024, and it's projected to increase to **$212B** in 2025 (Gartner).



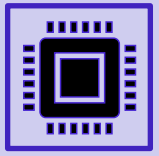
Spending + Technology = Better Security

Gartner Research: http://bit.ly/4hQKQZd

So, Why Doesn't Technology Alone Solve this Problem?

No company has the resources to fix every problem and mitigate every risk

Many companies don't know what assets they have; let alone the critical ones



Security Teams are often oblivious to how the business process works and how users use the technology

If the cybersecurity and risk teams don’t know the details of how the business works and its critical assets and processes, how can they ensure it is properly protected?

Created by: Chris Lau

RSAC™ 2025 Conference

Embracing Uncertainty

Know That You Can't Predict The Future

Many Voices.
One Community.

Assessing Risk

Making risk decisions can feel like a game of chess with so many variables that go into a risk decision or assessment score.

Does this really seem like the game we are playing?

Created by: Chris Lau

Nope, we're playing poker

Created by: Chris Lau

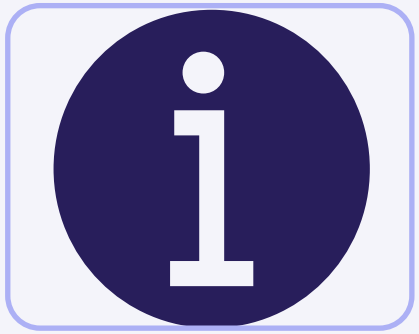
Embracing Uncertainty Like a Poker Player

Poker players make decisions that lead to their positive expected outcome – they know the future is unpredictable

Never judge the quality of the decision by the outcome.

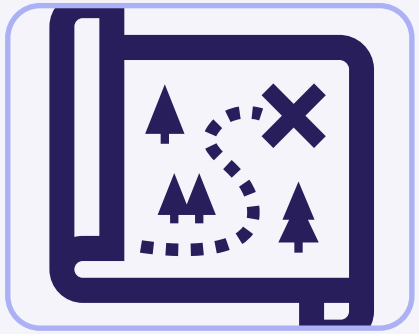
Created by: Chris Lau

Measuring Decision Quality

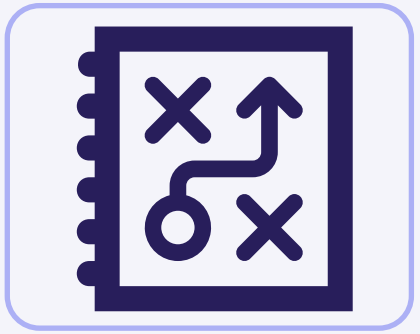


Hidden Information – what do we really know?

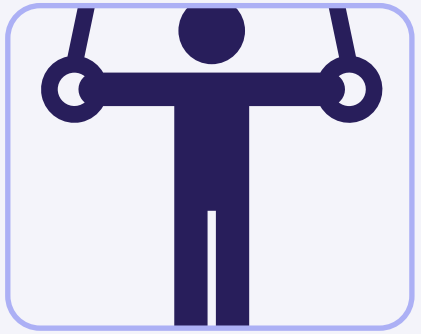
Previous Decisions – are they reliable?



Scenario Planning – have we weighed different outcomes?



Finding Solutions vs. Finding Obstacles



Adaptation – are we flexible based on data or rigid?

The Danger of Relying Solely on Past Performance

Created by: Chris Lau

Past successes (and failures) do not guarantee the future –

Learn from them, but don't rely solely on past performance.

Think Like an Attacker

Created by: Chris Lau

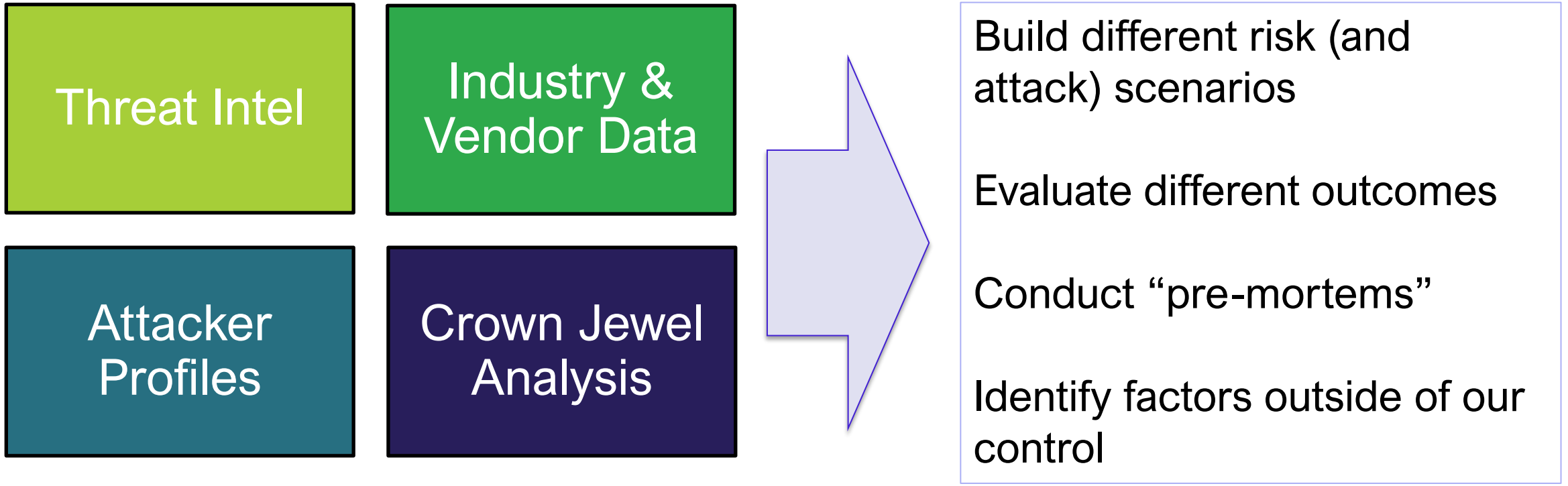
Compare the knowns and unknowns

Created by: Chris Lau

- Blind Spots – go beyond vulnerabilities
- Asset Inventory – hardware and software
- Understanding critical assets and the financial impact of an attack
- Deconstructing previous attacks and methods

Using Data to Think Like an Attacker

Think about strategic bets – build resiliency and turn your risk/security program into a competitive advantage.

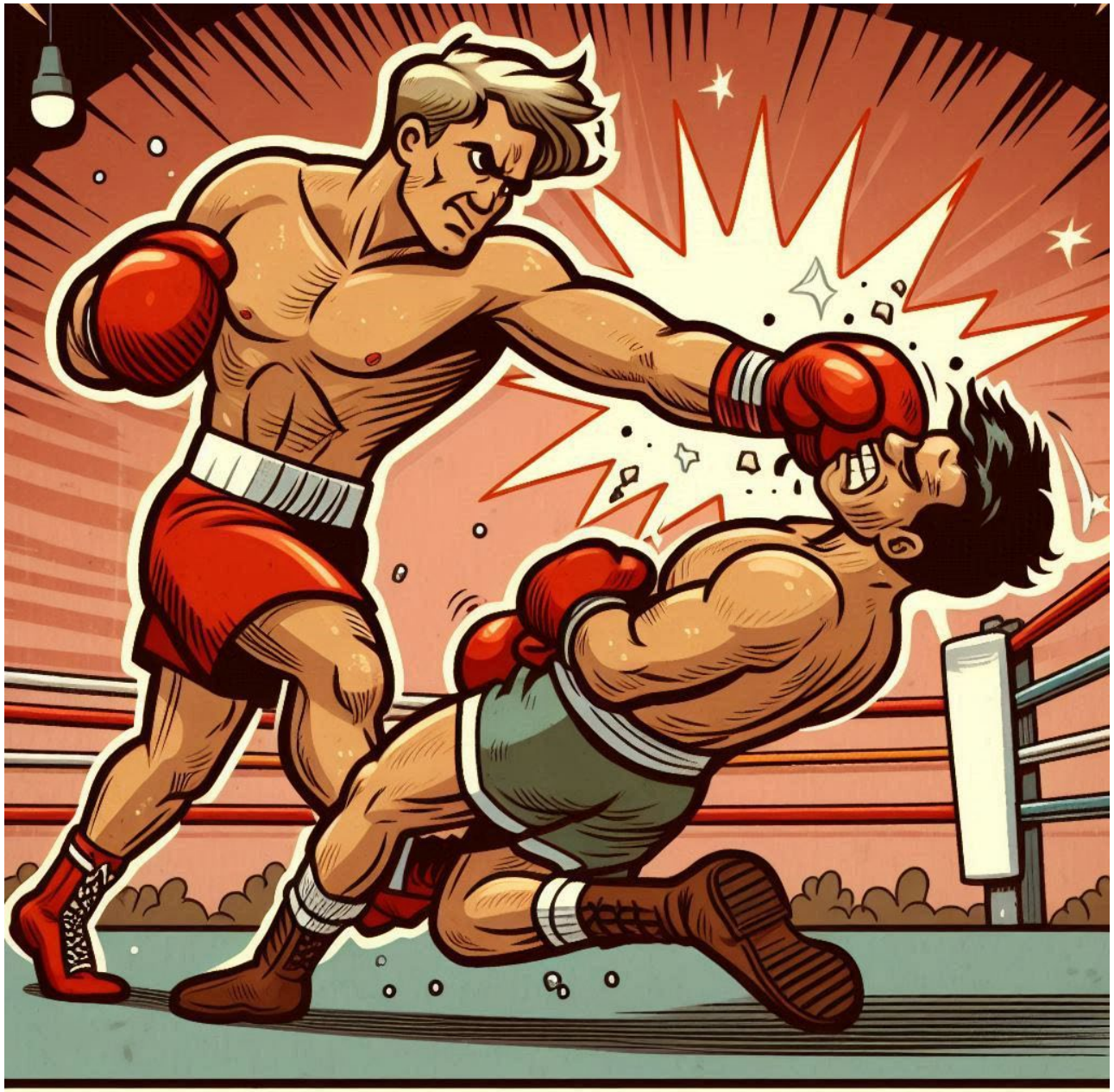


RSAC 2025 Conference

Proactive Security

Learning to Play Offense

Many Voices.
One Community.



Created by: Chris Lau

“Everyone has a plan until they get punched in the mouth.”

Mike Tyson

Changing the Risk Mindset

Once you link business process, strategic goals and the supporting technology, the risk picture becomes more focused:

What risks do we face?
How could a cyberattack impact our business?
Is our executive team engaged in prioritizing cybersecurity risks?
Are we investing in the right areas to defend ourselves?
Are our current defenses and controls effective?

The Evolution to Offense and Resiliency

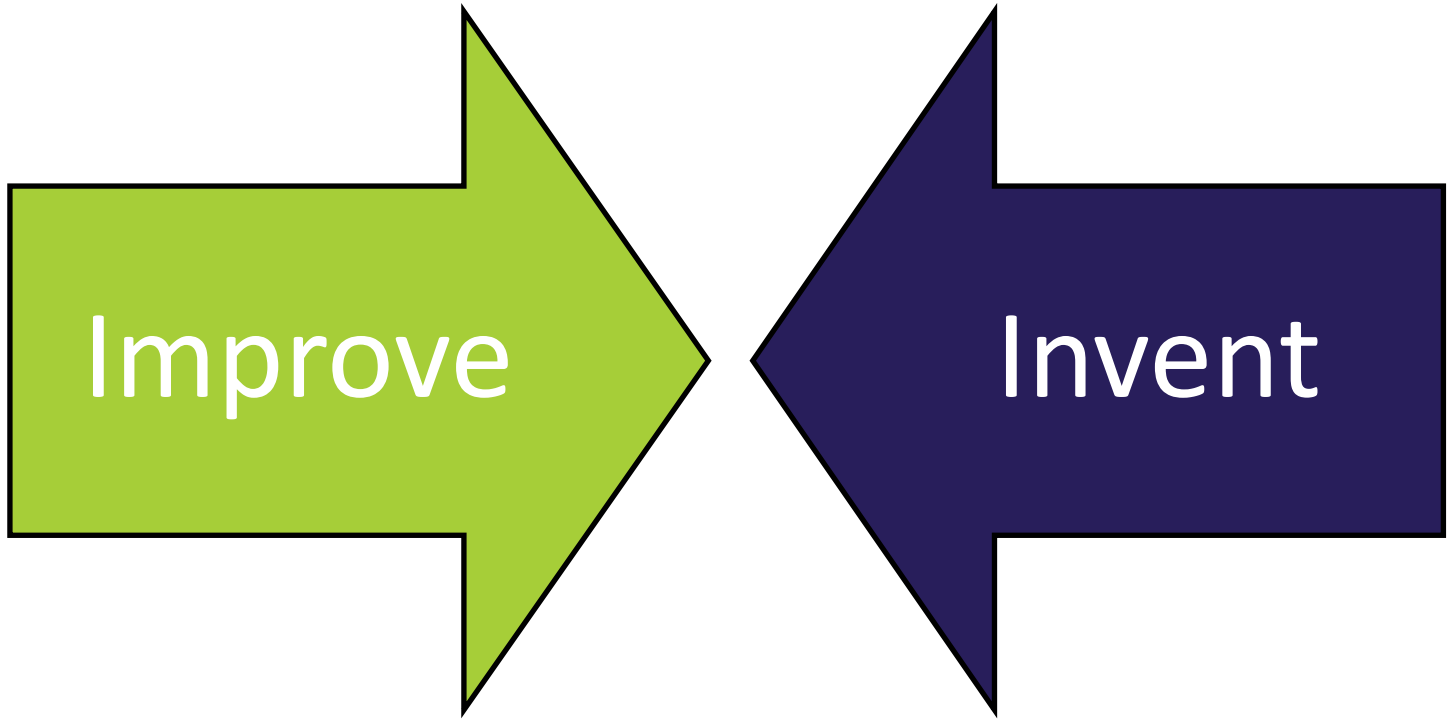
Created by: Chris Lau

We can’t continue to operate status quo while attackers evolve.

- Leadership Driven
- Forward Thinking
- Strategic and Execution Focused
- Building Resiliency

How we build resilience

Controls, processes, awareness



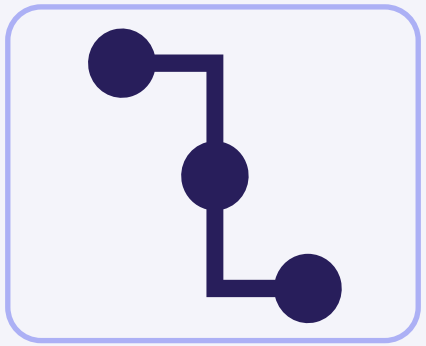
Adapt to ever-changing threats

Use data to understand the potential impact of realized risks.

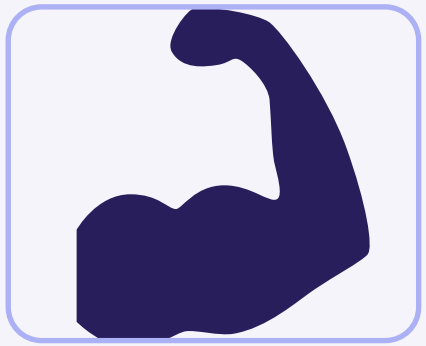
Real World Resiliency

Understand where the critical assets reside

Document system and process relationships



Create a simple process to evaluate risk, vulnerability impact, relevant threats, and likelihood

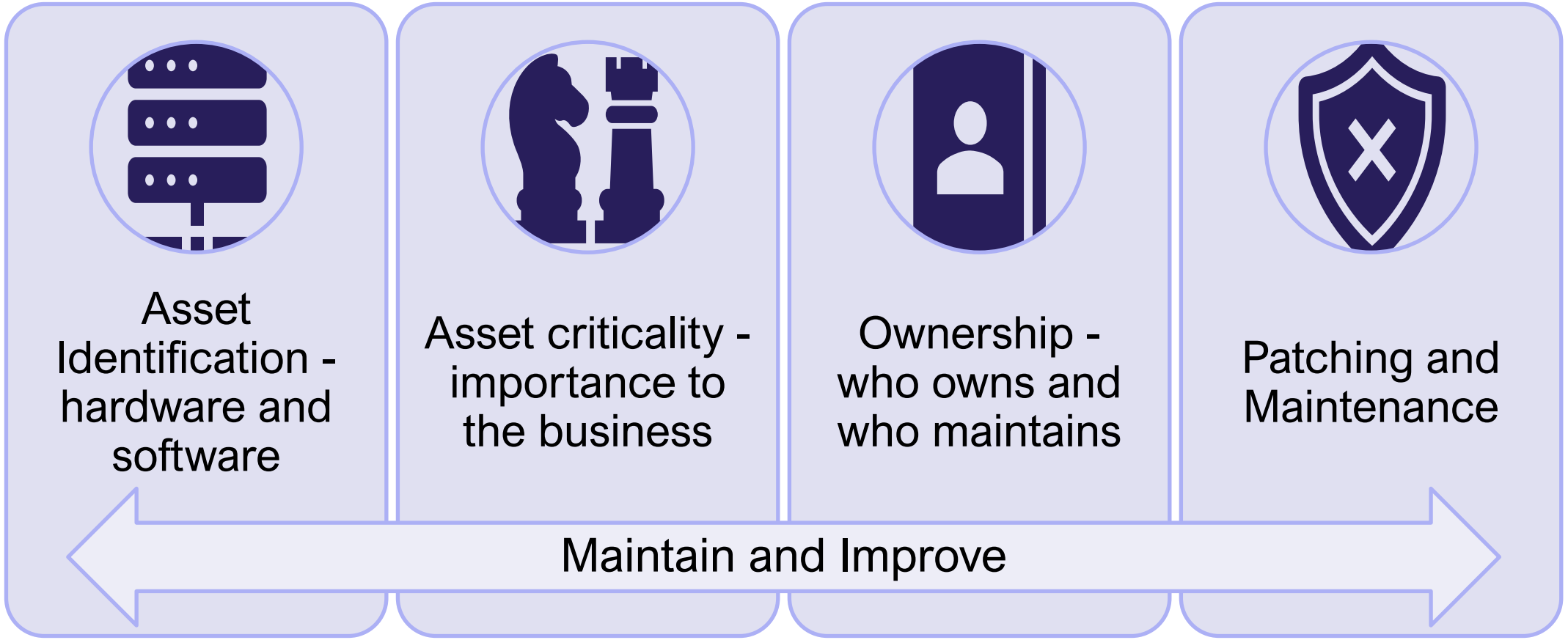


Build resiliency into critical business processes and systems

Establish clear communication about risk across all departments

Be World Class in the Basics

Sure, it's boring, but by focusing on the fundamentals, we can understand our business better than the attacker.


Asset Identification - hardware and software
Asset criticality - importance to the business
Ownership - who owns and who maintains
Patching and Maintenance
Maintain and Improve

Created by: Chris Lau

#RSAC

Traditional Vulnerability Management

RSAC 2025 Conference

Rethinking Vulnerability Management

By playing offense in vulnerability management, you can identify other exposures beyond the traditional CVSS focus that can reduce areas of risk proactively.

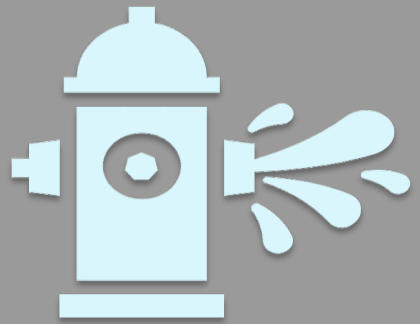
Places to Start

Known exploited vulnerabilities (KEVs)	Legacy | EOL Software	Default and weak creds	Overextended privileged access
Inadequate or insecure system configurations	Lack of policy enforcement	Blind Spots – visibility or device	Conduct pre-mortems – assess the impact BEFORE it happens

Context is Everything

Not every critical vulnerability may need to be patched or even addressed – asset and business context helps fill the gaps.

How easy is it to exploit?



What does a "bad day" look like for us?

What breaks if that happens?

How much do we lose?

RSAC™ 2025 Conference

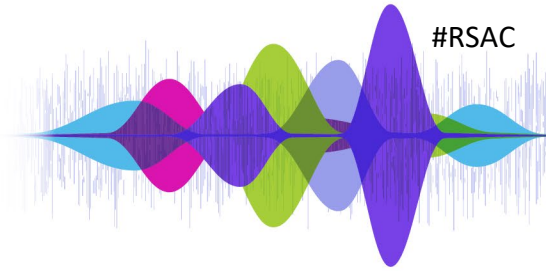
Apply

Many Voices.
One Community.

Crafting A Winning Hand

Created by: Chris Lau

Apply What You Learned Today



- Right Away:

  Conduct a baseline assessment of the entire program – be brutal and realistic.

  Identify blind spots in both assets and processes.

  Build a model to assess the financial impact of a successful risk event.

- Within 90 Days:

  Map critical assets and infrastructure – know data paths, dependencies, interconnections, etc..

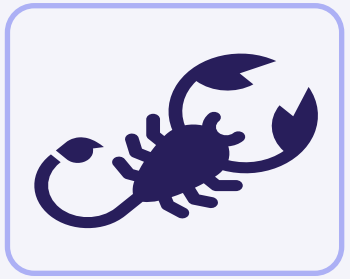
  Document asset ownership, patching scenarios, and schedules

  Establish new operating mechanisms that build lines of communication with executives and business teams.

Key Takeaways

Be comfortable being uncomfortable. You will never have perfect or complete information.

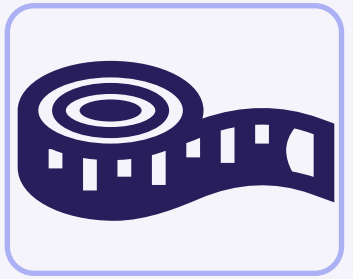
Use risk to inform protection



Adapt to ever-evolving threats

Balance progress with perfection

Stay connected to the business



Measure the right things

Be certain of **NOTHING**

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You !

www.linkedin.com/in/christopher-lau-mba